RITO
राजस्थान सूचना प्रौद्योगिकी संस्थान
Rajasthan Information Technology Organization

Cybersecurity Awareness in Rajasthan 2025

The Consumer Survey Report

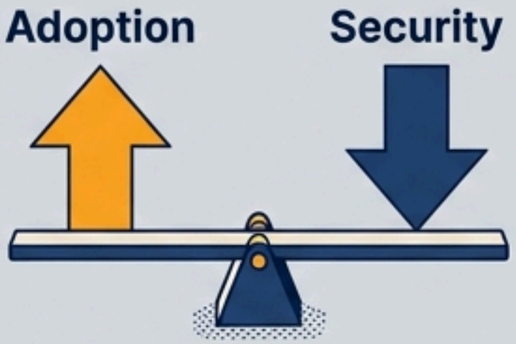
An empirical study of 10,000 citizens establishing the definitive baseline of digital security maturity in the region. Conducted solely by the Rajasthan Information Technology Organization.

Executive Summary

The RITO Security Blueprint

10,000 Respondents

A proprietary statewide database capturing insights across corporate environments, trade associations, and public campaigns.



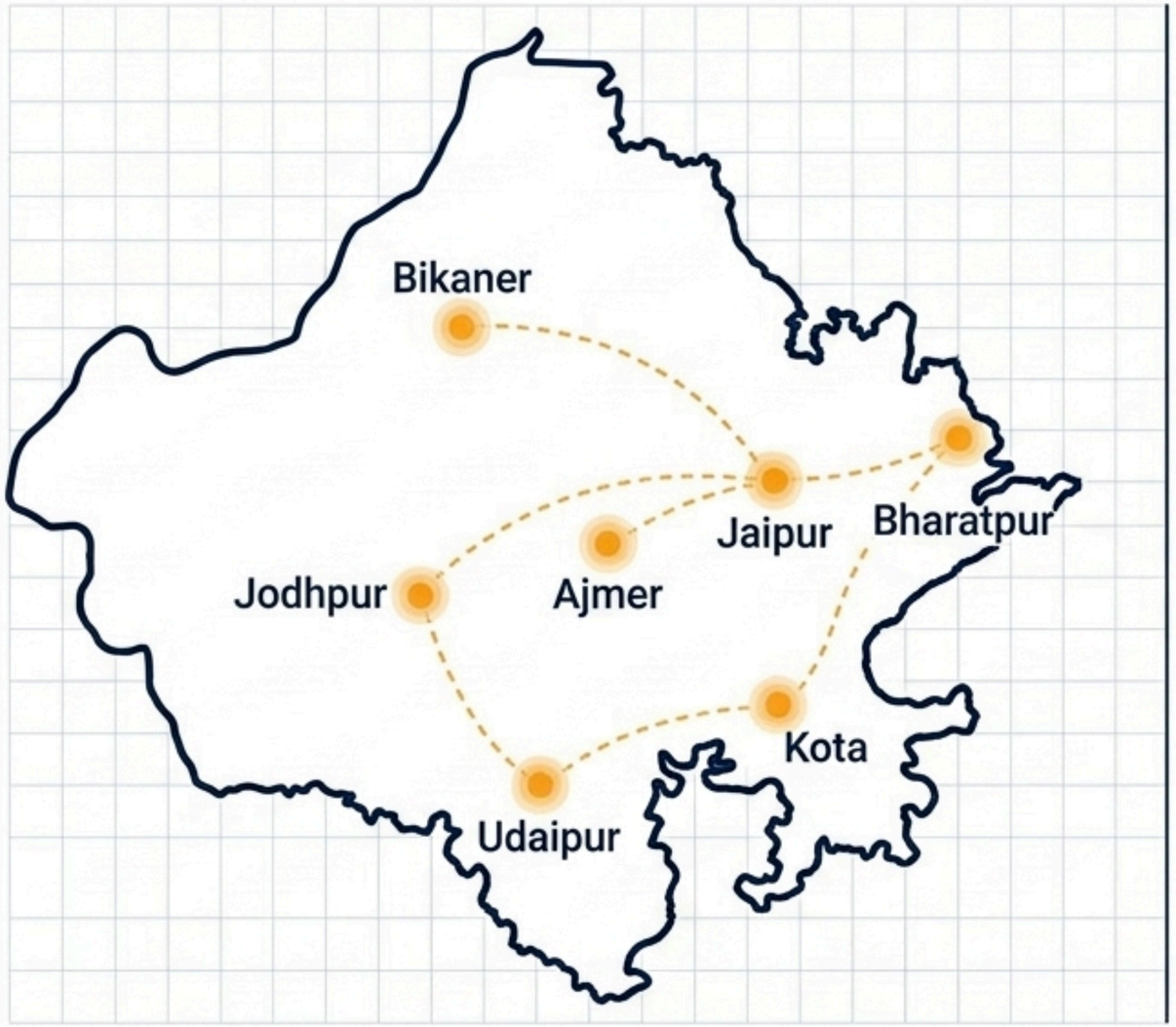
The Core Finding

Digital adoption—such as UPI, cloud computing, and remote workflows—has hit widespread saturation (>88%), but operational cyber hygiene remains a critical, lagging vulnerability.

The Action

Moving Rajasthan from basic digital adoption to robust digital resilience through targeted initiatives, SME audits, and continuous corporate simulations.

Methodology & Sample Composition



N = 10,000 Respondents

35% (3,500) Corporate & IT Enterprise Employees

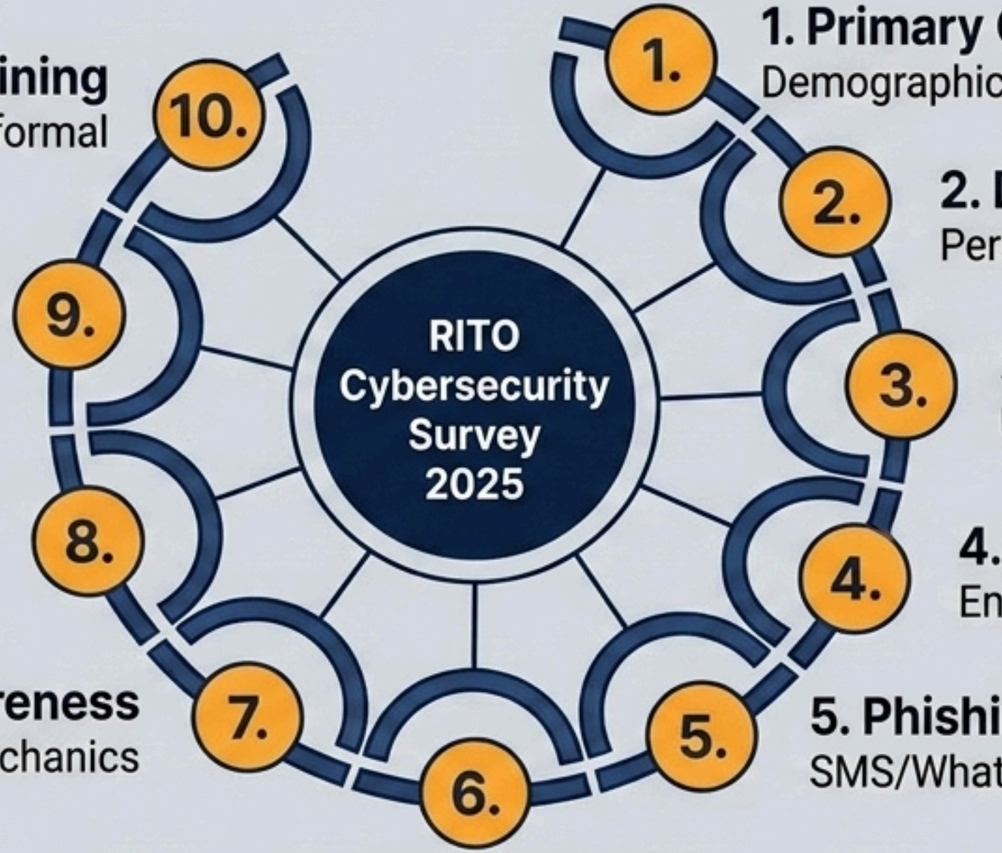
25% (2,500) Trade Associations & MSME Business Owners

25% (2,500) Public Campaign & Event Participants

15% (1,500) Students & Educational Stakeholders

The 10-Point Survey Architecture

Validating empirical data through a rigorous, proprietary questionnaire.



1. Primary Category
Demographics

2. Device Usage
Personal/Corporate/Shared

3. Password Management
Update frequency/Reuse

4. MFA Enrolment
Enforcement levels

5. Phishing Exposure
SMS/WhatsApp frequency

6. Link Verification
Inspection habits

7. UPI PIN Awareness
Debit vs. Receive mechanics

8. Public Wi-Fi Safety
VPN usage

9. Cyber Incident Action
Reporting channels

10. Organizational Training
Formal vs. Informal

Synthesis: The Adoption-Security Gap

The Adoption-Security Gap

Digital Adoption Saturation (UPI, Cloud, Remote Workflows)

Corporate MFA Enforcement

Rapid Incident Reporting

Phishing Click-Through Rate

The Adoption-Security Gap: Rajasthan's citizens possess the tools of the digital economy, but lack the operational hygiene required to defend their assets.

Pillar 1: Authentication hygiene drops sharply outside corporate environments

52%

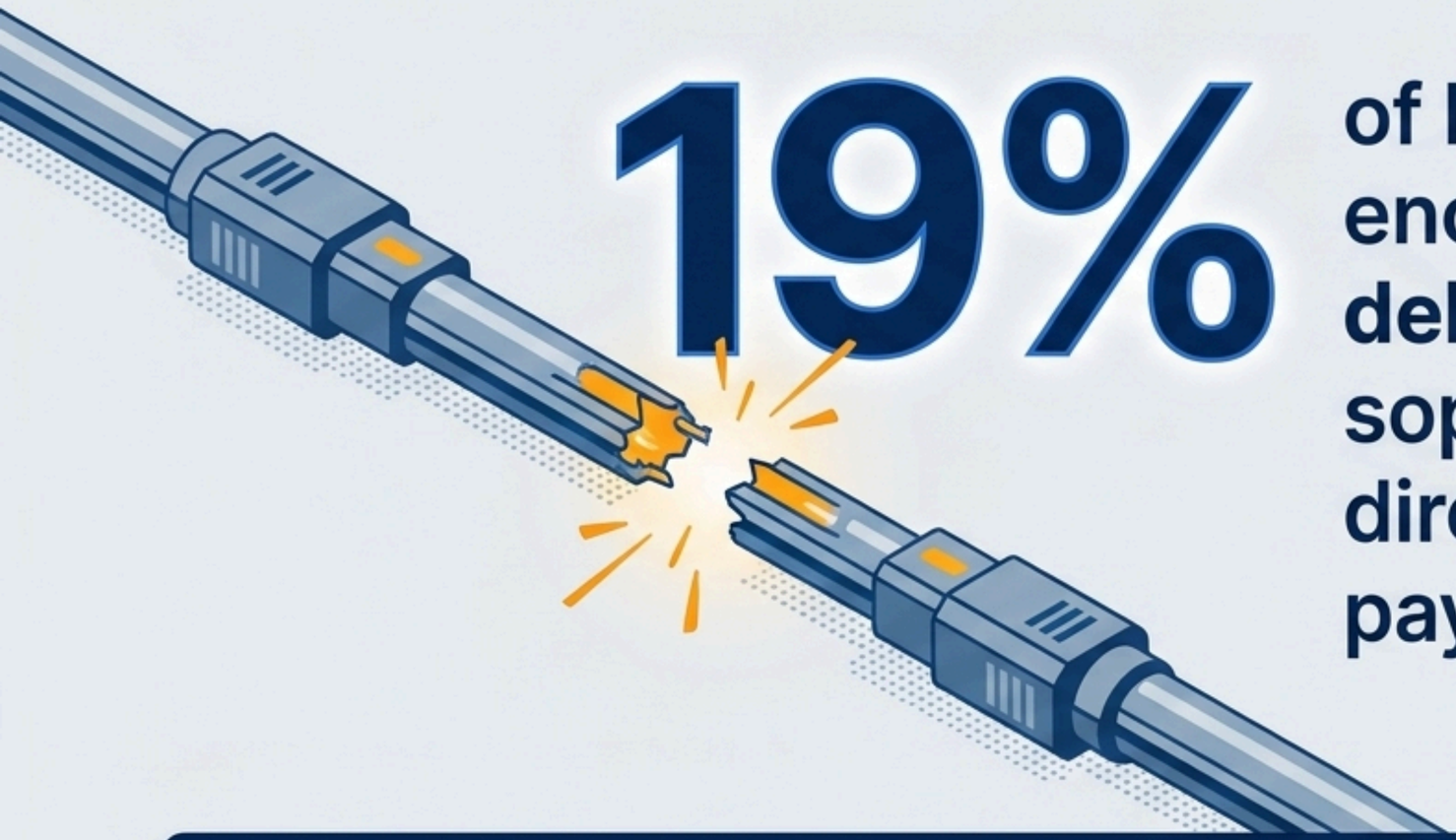
Over half of respondents reuse the same password across multiple personal and work accounts, creating a cascading risk for enterprises.

Multi-Factor Authentication (MFA) Enrolment

Insight: Even in controlled corporate environments, MFA enforcement fails to reach 40%, leaving widespread systemic vulnerabilities.

Pillar 2: MSMEs face sustained attacks on digital financial infrastructure

ALERT



19% of MSMEs reported encountering **unauthorized debit attempts** or sophisticated **phishing links** directly targeting their payment gateways in 2025.

Takeaway: As trade associations digitize, attackers are pivoting from consumer scams directly to B2B payment friction points.

The UPI Misconception: Reversing the Flow of Funds

62% correctly understand entering a PIN is strictly for paying out.

38% dangerously believe a PIN is required to receive funds.

Legitimate Transaction

Enter PIN

Money Leaves Account

Reverse-Charge Scam

Scammer sends payment link

Victim prompted for PIN

Entering a PIN never pulls money in; it only authorizes a debit.

The RITO Security Blueprint

Pillar 3: Omnichannel threat exposure penetrates all demographics

71%

Received fake electricity bill, lottery, or urgent job scam messages via WhatsApp and SMS in 2025.

44%

Corporate phishing click-through rate. Nearly half of corporate participants clicked on an untrusted email link or WhatsApp file during the year.

The Demographic Divide: Assessing Vulnerability Profiles

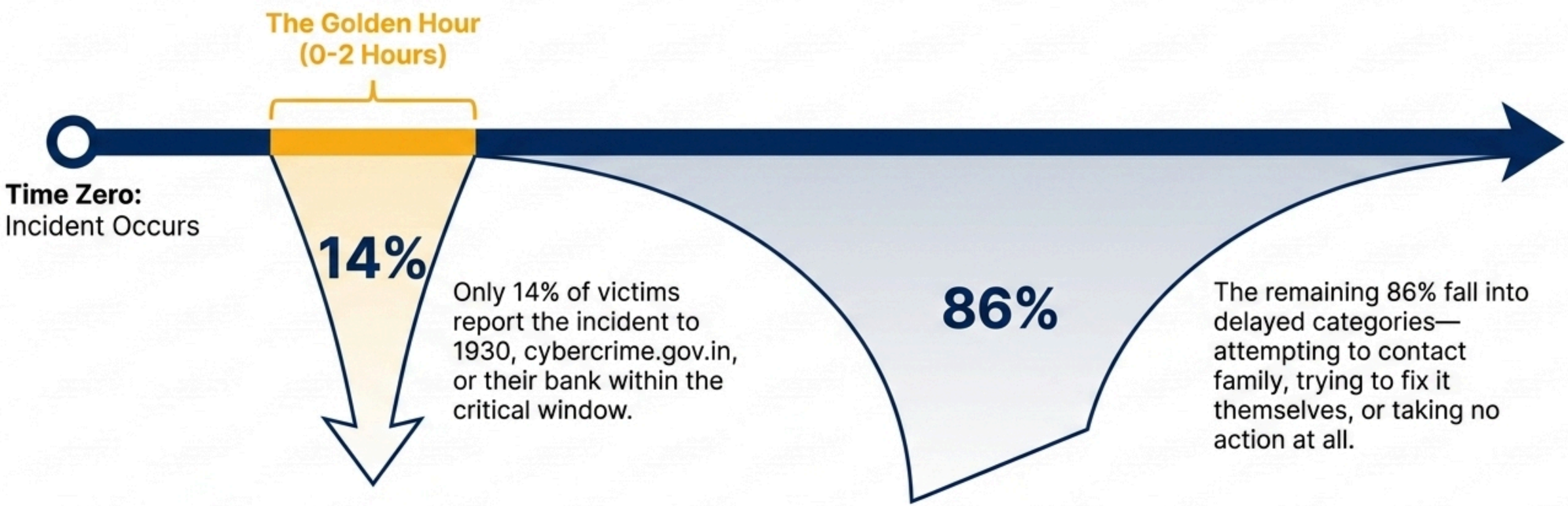
	Authentication	Phishing Susceptibility	Helpline Awareness
Corporate Workforce	38% MFA Enforcement	44% Click Rate (Critical)	54% in Tier-1 Hubs
MSME / Trade	18% MFA Enrolment	Targeted via Payment Gateways	Moderate Recognition
Tier-3 / Rural Citizens	12% MFA Enrolment	Highly Exposed to WhatsApp Scams	29% Recognition

The RITO Security Blueprint

Pillar 4: Geographic decay in incident response awareness

The physical distance from major tech hubs directly correlates with a dangerous isolation from emergency digital reporting infrastructure.

The "Golden Hour" Deficit: Reporting Velocity



Delayed reporting renders financial recovery mechanisms and account freezing protocols almost entirely ineffective.

RITO Strategic Action Plan: Protecting Trade and the Public

Initiative 1

RITO SME Cyber Shield Initiative

Target: Trade associations and MSMEs.

Action: Establish dedicated cybersecurity audits and hands-on Multi-Factor Authentication (MFA) deployment assistance programs specifically for small businesses.

Initiative 2

Vernacular Cyber Safety Campaigns

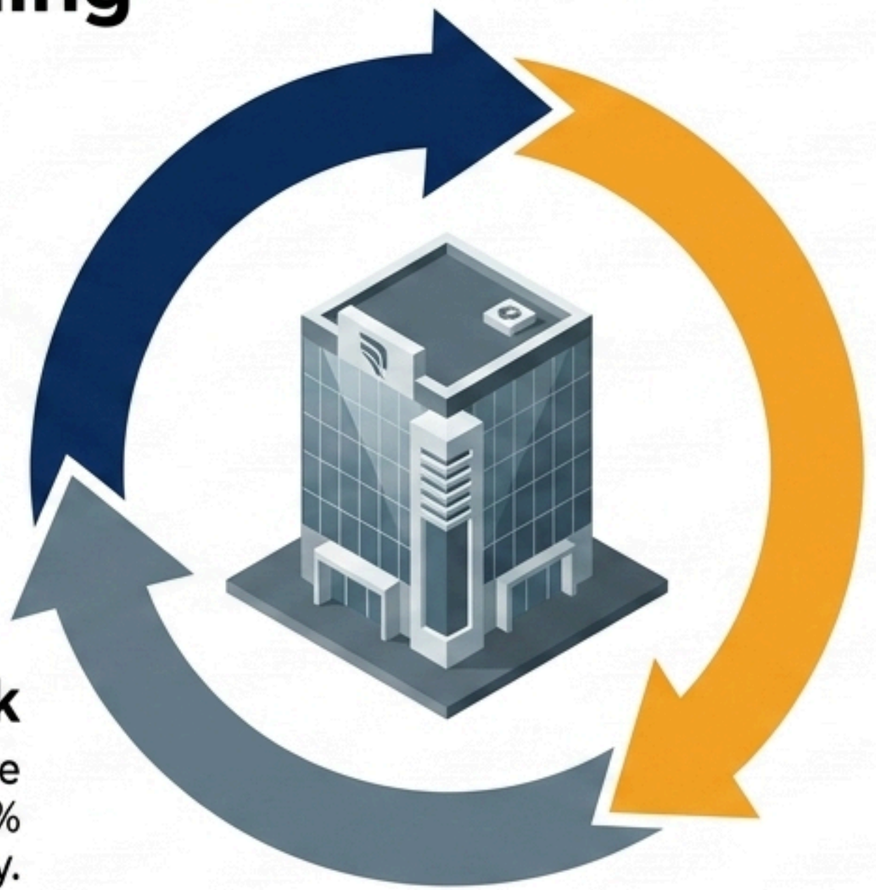
Target: General public and Tier-3 / Rural citizens.

Action: Produce multi-channel Hindi and Rajasthani video guides explicitly explaining UPI PIN mechanics and deconstructing fake bill and lottery scams.

RITO Strategic Action Plan: Enterprise Hardening

Step 1: Partner

Partner with Rajasthan enterprise hubs and corporate sectors.



Step 2: Execute

Execute quarterly phishing benchmark simulations on employees.

Step 3: Track

Track compliance and measure the reduction in the current 44% click-through vulnerability.

Transforming organizational training from informal, annual checkboxes into a continuous, metric-driven security culture.

RITO

राजस्थान सूचना प्रौद्योगिकी संस्थान

Rajasthan Information Technology Organization

Building the digital resilience of Rajasthan, one citizen at a time.

Access the full proprietary database, request a corporate audit, or explore vernacular campaign resources online.

https://rito.org.in/

Published 2025 | Rajasthan Information Technology Organization (RITO)